Модельная программа
Школы Цифровых Прав

Основы функционирования сети Интернет: технические аспекты

- как функционирует интернет: многоуровневость интернета, система IP-адресов и доменных имен, DNS;
- кто за что отвечает в Интернете: регистраторы, ISP и хостинг-провайдеры, пользователи и владельцы сайтов;
- интернет национальный и наднациональный: как соотносится построение и регулирование Интернета и государственные границы;
- киберпреступность: национальные и международные подходы к регулированию.

Состояние киберпространства Кыргызской Республики

- противоправные действия в киберпространстве;
- инциденты;
- роль и значение центров реагирования на компьютерные угрозы**.**

Кибербезопасность

- что такое политика кибербезопасности?
- лучшая практика по национальным стратегиям по кибербезопасности.

Криптография и электронная подпись в киберпространстве

- симметричная и асимметричная криптография;
- применение криптографических технологий в Интернете (https, IPSec, VPN);
- криптография и электронная подпись;
- организация криптообмена: двусторонний обмен, доверенная третья сторона и единое пространство доверия;
- функционирование инфраструктуры открытых ключей на национальном и наднациональном уровне.

Электронное управление

- задачи и последствия перехода к электронному управлению;
- основные элементы инфраструктуры электронного правительства.

Технические аспекты перехода к оказанию государственных услуг в электронном виде

- ИКТ инфраструктура государственных органов Кыргызской Республики (роль и значение элементов, технические стандарты, ЦОДы, GCould);
- X-Road: техническое взаимодействие при оказании государственных услуг;
- роль и значение технических стандартов информационной безопасности;
- ИКТ инфраструктура Евразийского экономического союза (вызовы, решения).

Переход к электронному управлению

- стандарты электронных государственных услуг (как создаются стандарты, регламенты);
- правовое обеспечение перехода к электронному управлению;
- стандарты информационной безопасности.

Электронное управление

- базовые информационные ресурсы: что к ним относить, как осуществлять управление базовыми информационными ресурсами? Объединение и разделение базовых информационных ресурсов;
- защита информации в информационных системах. Модель угроз, модель нарушителя, уровни защищенности и способы их достижения. Регуляторные подходы к обеспечению защиты информации в информационных системах: формальный и риск-ориентированный.

Регулирование Интернет

- понятие "управления Интернетом": что в него вкладывается, какие подходы существуют. История управления Интернетом;
- слои (уровни, корзины) в Интернете: инфраструктура и стандартизация; право; экономика; развитие; социокультурные аспекты;
- участники процесса управления Интернетом: государство, бизнес, гражданское общество, международные организации, Интернет-сообщество и ICANN.

Персональные данные и защита частной жизни

- история вопроса;
- основные подходы к защите частной жизни в мировой практике.

Персональные данные: система законодательства

- понятие и категории персональных данных;
- принципы и условия обработки персональных данных;
- субъекты, осуществляющие обработку;
- независимый надзорный орган;
- обеспечение безопасности данных;
- трансграничная передача;
- ответственность за нарушения в области персональных данных.

Технические и юридические аспекты при осуществлении надзора за доступом к персональным данным:

- доступ к ПД;
- вопросы защиты ПД при их обработке в информационных системах;
- обеспечение безопасности хранения и использования ПД;
- надзор (в том числе техническими средствами);
- защита прав субъектов ПД.

Правовые и технические основы защиты критической инфраструктуры

- что такое критическая инфраструктура;
- организационно-технические мероприятия для защиты критической инфраструктуры;
- правовое обеспечение защиты критической инфраструктуры.